PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-191402
(43)Date of publication of application : 30.07.1993

(51)Int.Cl. H04L 9/22
G09C 1/00
H04L 9/06
H04L 9/14

(21)Application number : 04-003670
(22)Date of filing : 13.01.1992

(71)Applicant : HITACHI LTD
(72)Inventor : FUKUZAWA YASUKO
TAKARAGI KAZUO
NAKAMURA TSUTOMU
HIRANO SHUICHI

(54) GENERATING SYSTEM FOR ASYMMETRICAL CIPHERING KEY

(57)Abstract:
PURPOSE: To facilitate the management and operation by generating an open key from information specific to a computer so as to register only the specific information and the open key to a center thereby reducing a verification time of the open key by the center.
CONSTITUTION: An open key of an asymmetrical ciphering key is generated from open identification information specific to a computer possessing a key or a person possessing a key. Thus, since the identification information specific to the possessor of the key or the computer possessing the key is verified from an open key of the asymmetrical ciphering key, it is not required to verify the open key with the center. Thus, the data to be verified by the center is the open key and the specific information of the key possessor or the computer possessing the key and the open key is eliminated from the data to be verified by the center.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－191402

(43)公開日　平成５年(1993)７月30日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/22				
Ｇ０９Ｃ　1/00		9194－5L		
Ｈ０４Ｌ　9/06				
		7117－5K	Ｈ０４Ｌ　9/ 04	
		7117－5K	9/ 02	Ｚ

審査請求　未請求　請求項の数９(全　８　頁)　最終頁に続く

(21)出願番号　特願平4－3670

(22)出願日　平成４年(1992)１月13日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　福澤　寧子
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　中村　勤
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

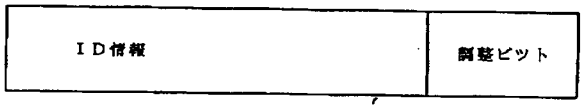
(54)【発明の名称】　非対称暗号鍵の生成方式

(57)【要約】

【目的】非対称鍵暗号を用いた暗号化通信に不可欠な暗号鍵の生成において、公開情報から公開鍵を生成することで、センタによる公開鍵の認証時間を短縮し、管理、運用を容易にする。

【構成】非対称暗号鍵生成プログラム205による非対称暗号鍵の公開鍵（ｄ、ｎ）の生成において、計算機201に固有の情報209から公開鍵（ｄ）を生成することで、固有の情報と公開鍵（ｎ）だけをセンタに登録する。

図１



【特許請求の範囲】

【請求項１】第一の公開鍵ｄと、秘密鍵ｅとが、ｅ・ｄ≡１（ｍｏｄ　ｆ）の関係にあり、前記ｆの値が、第二の公開鍵をｎとしたとき、ｎ＝ｐ・ｑを満たす二つの素数ｐ，ｑに対して、ｆ＝ｌｃｍ（ｐ－１，ｑ－１）の関係（但し、ｌｃｍは最小公倍数を意味する）にあるような非対称暗号鍵の生成方式おいて、前記第一の公開鍵ｄの上位ビットに、鍵の所有者に固有の、または鍵を所有する計算装置に固有の情報を適用し、ｇｃｄ（ｄ，ｐ－１，ｑ－１）＝１の関係（但し、ｇｃｄは最大公約数を意味する）を満たすように、前記公開鍵ｄの下位ビットを調整することを特徴とする非対称暗号鍵の生成方式。

【請求項２】請求項１において、前記該第一の公開鍵ｄの上位ビットに、鍵の所有者に固有の、または鍵を所有する計算装置に固有の情報と、前記第二の公開鍵ｎの情報をハッシュ処理で変換した結果とを結合して適用し、前記秘密鍵ｅと、前記素数ｐ、ｑとの上記の関係を満たすように、前記公開鍵ｄの下位ビットを調整する非対称暗号鍵の生成方式。

【請求項３】請求項１または２において、前記第一の公開鍵ｄの上位ビットとして生成された値のうち、所定のビット数の値に応じて、予め設定されている比較的小さな素数を第一の公開鍵ｄとして決定する非対称暗号鍵の生成方式。

【請求項４】請求項１、２または３において、生成された前記第二の公開鍵ｎは、ｎの下位一ビットを取り除いたｎ－１ビット長のｎ'を前記第二の公開鍵ｎとして、予めシステムに設定されているセンタによって、センタの秘密鍵で、暗号化される非対称暗号鍵の生成方式。

【請求項５】前記第一の公開鍵ｎと、ｎ＝ｐ・ｑを満たす二つの素数ｐ，ｑを秘密鍵（ｐ，ｑ）とし、第二の公開鍵ｂが、０≦ｂ＜ｎの関係を満たすような非対称暗号鍵の生成方式おいて、前記第二の公開鍵ｂに、鍵の所有者に固有の、または鍵を所有する計算装置に固有の情報を適用することを特徴とする非対称暗号鍵の生成方式。

【請求項６】請求項５において、前記第二の公開鍵ｂに、前記鍵の所有者に固有の、または鍵を所有する前記計算装置に固有の情報と、前記第一の公開鍵ｎの情報をハッシュ処理で変換した結果を結合して適用し、前記公開鍵ｎとの関係を満たすように、前記第二の公開鍵ｄを生成する非対称暗号鍵の生成方式。

【請求項７】請求項１，２，３，４，５または６において、前記固有の情報として、利用者毎の識別情報や、計算機に予め設定されている固有の製造番号や通信アドレスを用いる非対称暗号鍵の生成方式。

【請求項８】請求項１，２，３，４，５，６または７において、前記計算機毎に固有の情報や前記鍵の所有者の識別情報を、計算機製造時に計算機内蔵ＲＯＭに書き込み、再設定ができない計算機である非対称暗号鍵の生成方式。

【請求項９】請求項１，２，３，４，５，６または７において、非対称暗号鍵生成部、および前記記憶手段は、前記計算機に着脱可能な回路装置により構成される非対称暗号鍵の生成方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、公開の固有情報を非対称暗号鍵の公開鍵として利用するものであり、非対称暗号鍵の生成方式に関する。

【０００２】

【従来の技術】通信ネットワークを介して、会議や種々の取引を電子的に行うビジネス通信の時代が始まり、情報セキュリティの必要性は増大しつつある。情報セキュリティを確保するための暗号技術の一つであるＲＳＡ暗号方式やＲＡＢＩＮ暗号方式等の非対称暗号鍵暗号方式は、データ保護だけでなく、相手認証の機能を持つことから有用な暗号方式と考えられている。（ＩＤベース鍵生成機能の例：コーンフェルダー（Kohnfelder）の方法　出典：（株）昭昇堂発行、辻井重男、笠原正雄編著、「暗号と情報セキュリティ」pp94～）まず、ＲＳＡ暗号化鍵、復号化鍵の生成の基本手順を示す。

【０００３】ステップ１：十分大きな素数ｐ，ｑをランダムに選ぶ。ｐ，ｑは秘密にしておく。

【０００４】ステップ２：ｐ・ｑの積をｎとする。

【０００５】ステップ３：ｆ＝ｌｃｍ（ｐ－１，ｑ－１）とし、ｇｃｄ（ｄ，ｆ）＝１となる、ｆと互いに素な整数ｄをランダムに取出す。

【０００６】ここで、ｌｃｍ（ｘ，ｙ）は、ｘとｙの最小公倍数、ｇｃｄ（ｘ，ｙ）は、ｘとｙの最大公約数を示す。

【０００７】ステップ４：ｆを法として、ｅ・ｄ≡１（ｍｏｄ　ｆ）となる、ｄの逆数ｅを定める。

【０００８】上記の手順で暗号化鍵（ｅ、ｎ）、復号化鍵（ｄ、ｎ）が生成される。

【０００９】暗号化では、平文Ｍを０～（ｎ－１）までの間の整数Ｃに変換し、復号化では、暗号文Ｃを平文Ｍに変換する。

【００１０】暗号化

【００１１】

【数１】

$$C \equiv M^{e} \pmod{n}$$

【００１２】復号化

【００１３】

【数２】

$$M \equiv C^{d} \pmod{n}$$

【００１４】これは(ｍｏｄ　ｎ)において、積を何度も繰り返すと元に戻るという周期性に依存したアルゴリズムである。ＲＳＡ暗号方式では、暗号化鍵と復号化鍵は一対をなしており、（ｅ、ｎ）で暗号化されたものは（ｄ、ｎ）でしか復号化することができず、しかもｎの

値が五百ビット程度の長さ持つ場合には、（ｄ、ｎ）から（ｅ）を求めることは、ｎの素因数を知らなければ計算量的に大変困難であるという性質を持つ。

【００１５】ＲＳＡ暗号方式を用いて秘密通信を行う場合は、暗号化鍵を公開し、復号化鍵を秘密管理する。また、逆にディジタル署名を行う場合、暗号化鍵を秘密管理し、復号化鍵を公開にする。

【００１６】さて、名前や住所といった公開の識別情報（ＩＤ）そのものが、そのまま公開の暗号鍵（公開鍵）としての役目を果たすことができれば、公開鍵から鍵の所有者を認証することができるので鍵管理は非常に容易になる。この考え方は1978年頃から提案されてきている。しかし、前述したように、公開の識別情報を非対称暗号鍵暗号方式の公開鍵としてそのまま用いることは、公開の識別情報が秘密鍵との関係を満たすとは限らないので、実現できない。そこで、従来例で示されるようなＩＤを用いた非対称暗号鍵証明配送方式が提案されている。これを以下に示す。

【００１７】（１）まず、図９に示すように、ユーザＡはユーザＡの公開情報（ID_A）と自身の公開鍵(d_A、n_A)を鍵管理機関であるセンタに登録する。

【００１８】（２）センタは、センタの秘密鍵（Ｓｃ）で暗号化したお墨付きの（センタによって認証された）ユーザＡの公開鍵をユーザＡに渡す。

【００１９】ユーザＡのお墨付き公開鍵：RSA_{Sc}（ID_A、d_A、n_A）

（３）次に、図10に示すように、ユーザＡと暗号通信を行いたいユーザＢは、お墨付きのユーザＡの公開鍵をユーザＡより受取り、センタの公開鍵（Ｐｃ）で復号化する。

【００２０】

RSA_{Pc}（RSA_{Sc}（ID_A、d_A、n_A））

（４）復号化した結果、ユーザＡのID_Aが正しい公開情報であることを確認できたら、公開鍵（d_A、n_A）も正しいものであるとし、以下、公開鍵（d_A、n_A）でメッセージを暗号化し、ユーザＡと暗号通信を行なう。

【００２１】このようにすれば、公開の識別情報から公開鍵を生成していないので、公開鍵から相手を認証することはできないが、公開の識別情報と公開鍵の関係をセンタによって認証（保証）されたことになる。

【００２２】

【発明が解決しようとする課題】Kohnfelderの非対称暗号鍵証明配送方式は、安全性の面からも有効であると考えられている。しかし、センタの秘密鍵で暗号化する必要のあるデータは、利用者毎にID_j、d_j、n_jであり、三ブロックの暗号処理が必要になる。暗号化通信を行うシステムの規模をm端末と想定すると、センタはセンタの秘密鍵で（３×ｍ）ブロックの暗号処理を行う必要がある。従って、暗号化する必要のあるデータ長を短くし、暗号処理のブロック数を減らすことは有効となる。

【００２３】

【課題を解決するための手段】上記問題を解決するために、本発明では次の手段を用いる。

【００２４】（１）鍵を所有する個人、あるいは鍵を所有する計算機に固有の公開の識別情報から非対称暗号鍵の公開鍵（ｄ）を生成する。

【００２５】（２）公開の識別情報から生成できない非対称暗号鍵の公開鍵（ｎ）だけを、センタの秘密鍵で暗号化し、認証する。前述したように、ＲＳＡ暗号方式は、ｎの素因数分解の計算量的な困難さに依存した方式であることから、公開鍵（ｎ）を公開の識別情報から生成するとｎの素因数分解の困難性が保証されない。従って、公開鍵（ｎ）を公開の識別情報から生成することはできない。

【００２６】

【作用】上記の手段により、次のような作用が生じる。

【００２７】非対称暗号鍵の公開鍵（ｄ）から、鍵の所有者、あるいは鍵を所有する計算機に固有の識別情報を認証することができるので、センタによって公開鍵（ｄ）を認証する必要が無い。従って、センタによって認証すべきデータは、公開鍵（ｎ）と鍵の所有者、あるいは鍵を所有する計算機の固有情報であり、公開鍵（ｄ）をセンタによって認証すべきデータからはずすことができる。

【００２８】

【実施例】図１～図８において、本方式の実施例を示す。

【００２９】〈実施例１〉図２は、本実施例のシステム構成を示す図である。

【００３０】センタであるホスト計算機209、ユーザの計算機（端末）201、205が通信網２００を介して結ばれている。センタは鍵管理機関としての役目を果たす。ユーザ計算機２０１は、内部に暗号機構202を持ち、センタの公開鍵204はＦＤ203に格納されている。同様に、ユーザ計算機205は、内部に暗号機構206を持ち、センタの公開鍵204はＦＤ207に格納されている。ホスト計算機209は、内部に暗号機構210を持ち、ユーザの公開鍵212、213が鍵ファイル211に格納される。センタの秘密鍵214は、センタのホスト計算機だけが参照できる。

【００３１】計算機（端末）201のユーザＡが公開鍵をセンタ209に登録し、計算機（端末）201のユーザＡと205のユーザＢが暗号通信を行うまでを以下に示す。

【００３２】図４は、本実施例のユーザの計算機のハードウェア構成を示す図である。

【００３３】計算機201は、ディスプレイ402とキーボード403からなる。計算機201上の暗号機構202は、メモリ404とＣＰＵ406から成り、メモリ404に格納されている非対称暗号鍵生成プログラム405で、ユーザＡの固有情報409から非対称暗号鍵を生成する。固有情報409とは、名

前や住所や通信アドレス等の固有の情報であり、かつ誰からも参照可能な情報である。生成された非対称暗号鍵は公開鍵と秘密鍵であり、秘密鍵はＩＣカードR／W407を介して、ＩＣカード408に格納し、メモリ404上にそのままの形で保管しない。公開鍵は、メモリ404上一時保管し、センタ209に登録し、センタによって認証された形でオンラインで配布するか、秘密鍵格納用のＩＣカードとは別のＩＣカード、あるいはＦ．Ｄ．等に格納して、配布する。

【００３４】以下、図５において、計算機201上で行う非対称暗号鍵生成処理（ＲＳＡ暗号鍵生成処理）について示す。

【００３５】ステップ 501：始め。

【００３６】ステップ 502：素数ｐを生成する。

【００３７】ステップ 503：素数ｑを生成する。

【００３８】ステップ 504：固有情報409から、公開鍵ｄを生成する。

【００３９】ステップ 505：ｐ，ｑ，ｄから次ぎの条件を満たすように、鍵ｅ，ｎを生成する。

【００４０】ｎ＝ｐ・ｑｆ＝ｌｃｍ（ｐ－１、ｑ－１）
ｅ・ｄ≡１（ｍｏｄ　ｆ）

ステップ 506：固有情報409と、公開鍵（ｎ）をセンタによって認証する。

【００４１】ステップ 507：終わり。

【００４２】この手順で、公開鍵ｄを生成する処理Ｆ（ステップ 504）を図６に示す。

【００４３】ステップ 601：始め。

【００４４】ステップ 602：奇数乱数を生成する。

【００４５】ステップ 603：固有情報409を上位ビットとし、奇数乱数を下位ビットなるように接続する。ただし、ｄ’＜ｎ。

【００４６】ｄ’＝固有情報　||　奇数乱数

ステップ 604：ｄ’が素数であるかどうかを判定する。素数であれば、ステップ606へ進む。素数でなければ、ステップ605へ進む。

【００４７】ステップ 605：奇数乱数に２を加える。ステップ603へ進む。

【００４８】ステップ 606：ｄ’をｄとして出力する。

【００４９】ステップ 607：終わり。

【００５０】出力される公開鍵ｄの形態を図１に示す。また、固有情報毎に処理Ｆの結果は常に一定である。

【００５１】この手順で、公開鍵ｎをセンタに登録する処理（ステップ 506）を図７で示す。

【００５２】ステップ 701、ステップ 701’：始め。

【００５３】ステップ 702：計算機201の公開鍵（n_A）と固有情報（ID_A）409をセンタのホスト計算機209に送る（手配送、あるいは別途暗号化して送る）。

【００５４】ステップ 703：ホスト計算機では、公開鍵（n_A）と固有情報（ID_A）をセンタ秘密鍵（Sc）214を用いて、暗号機構210によってＲＳＡ暗号方式によって暗号化し、センタによって認証された情報Ｃを生成する。

【００５５】$C=RSA_{Sc}$　（ID_A、n_A）

ステップ 704：公開鍵（n_A）と固有情報（ID_A）を鍵ファイル211のエリア212に格納する。

【００５６】ステップ 705：センタによって認証された情報Ｃを計算機201のユーザＡに配布する。ステップ 706：計算機201はセンタによって認証された情報Ｃをメモリ404に格納する。ステップ 707、ステップ 707’：終わり。

【００５７】ただし、センタによって認証された情報（Ｃ）の生成を、$C=RSA_{Sc}$　（ID_A、d_A、n_A）として、センタによって三ブロックの暗号化で行ったとしても、公開鍵（d_A）から固有情報（ID_A）を認証する効果がある。

【００５８】次に、ユーザＡ（計算機201）とユーザＢ（計算機205）が暗号通信を行う処理を図８で示す。

【００５９】ステップ 801、ステップ 801’：始め。

【００６０】ステップ 802：計算機205に、センタによって認証された情報（Ｃ）と公開鍵（d_A）を配送する。

【００６１】ステップ 803：ＦＤ207内のセンタの公開鍵（Pc）204を用いて、暗号機構206によって情報Ｃを復号化する。

【００６２】ID_A、$n_A=RSA_{Pc}$　（Ｃ）

ステップ 804：復号化結果の固有情報（ID_A）が正しければ、ステップ 805に進む。正しくなければ、ステップ 806に進む。

【００６３】ステップ 805：（d_A、n_A）を用いて、暗号通信を計算機201と計算機205で行う。

【００６４】ステップ 806、ステップ 806’：終わり。

【００６５】〈実施例２〉実施例１と同様手順で、ＲＡＢＩＮ暗号化鍵生成を行う。

【００６６】ＲＡＢＩＮ暗号化鍵は、二つの大きな素数ｐ，ｑを選び、その積を計算する。次に０≦ｂ＜ｎになるｂを定める。この時、公開鍵は（ｎ，ｂ）であり、秘密鍵は（ｐ，ｑ）となる。

【００６７】ステップ 501’：始め。

【００６８】ステップ 502’：素数ｐを生成する。

【００６９】ステップ 503’：素数ｑを生成する。

【００７０】ステップ 504’：固有の情報409を鍵ｂとする。

【００７１】ステップ 505’：ｐ、ｑから鍵ｎを生成する。

【００７２】ｎ＝ｐ・ｑステップ 506’：終わり。

【００７３】〈変形例１〉図３は、図６の処理で生成される公開鍵（ｄ）の形態の他の例を示す。公開鍵（ｄ）は、固有の情報と、公開鍵（ｎ）を一方向性関数ｈ（ハッシュ関数）によって処理した結果ｈ（ｎ）と、ｄを素数にするための調整ビットから成る。公開鍵（ｄ）と

（ｎ）の組合せを確認することが可能になる。

【００７４】〈変形例２〉センタのＲＳＡ暗号秘密鍵Ｓｃ＝（ｅC、ｎC）とすると、センタでユーザの公開鍵（ｎ）を認証するためには、ｎC＞ｎでなければならない。

【００７５】そこで、ユーザの公開鍵（ｎ）の最下位一ビットを取り除いたｎ’をセンタのＲＳＡ暗号秘密鍵で認証する。つまり、（ｄ、ｎ’）をセンタが認証する。実際に、ユーザの公開鍵（ｄ、ｎ）を用いて暗号通信を行う場合には、センタによって認証された公開鍵（ｄ、ｎ’）のｎ’の最下位に１を付加し、（ｄ、ｎ）として暗号通信を行う。これは、ｎが二つの素数の積であることから、奇数である。従って、最下位ビットが１であることは自明である。

【００７６】この結果、ｎC＞ｎ、かつｎCとｎが同ビット長の値である場合には、センタによる認証が可能になる。

【００７７】〈変形例３〉実施例１で生成された公開鍵（ｄ）の所定のビット数の値に応じて、予め設定された比較的短い素数を、公開鍵（ｄ）として用いる。

【００７８】〈変形例４〉以上は、計算機上のプログラムによる処理を前提としているが、図５～図８の演算の一部、あるいは全部を専用ハードウェア化することで実現することもできる。

【００７９】〈変形例５〉計算機固有の情報とは、計算機据付時に、端末利用ユーザによって入力されたデータを非公開の関数（時刻データ等をパラメータとして用いることで、意図的に値を生成できないような関数）で変換、生成した一意のコードや、予め計算機製造時に割当てられた固有の製造番号や、通信アドレス等を用いる。また、通信端末内のＲＯＭに製造段階で書き込んでおく。ＲＯＭに製造段階で書き込まれることによって、ユーザが意識的に書き直すことができない。

【００８０】

【発明の効果】本発明により、次のような効果が得られる。

（１）センタによって認証すべきデータは、公開鍵（ｎ）と鍵の所有者、あるいは鍵を所有する計算機の固有情報にすることが可能となり、公開鍵（ｄ）をセンタによって認証すべきデータからはずすことができるので、ユーザ毎の認証すべきデータを３ブロックから二ブロック以下にすることができる。従って、暗号化通信を行うシステムの規模をｍ端末と想定すると、センタはセンタの秘密鍵による暗号処理を、（３×ｍ）ブロックから（２×ｍ）ブロックに短縮できる。

（２）非対称暗号鍵の公開鍵（ｄ）から、計算機、あるいは個人の固有情報を認証することができる。

（３）公開鍵（ｄ）の一部に、公開鍵（ｎ）の圧縮データを組み入れることで、公開鍵（ｄ）と公開鍵（ｎ）の組み合わせを認証することができる。

（４）ユーザの公開鍵（ｎ）の最下位一ビットを取り除いたｎ’をセンタのＲＳＡ暗号秘密鍵で認証することで、センタのＲＳＡ暗号鍵（ｎC）とユーザの公開鍵（ｎ）がｎC＞ｎでも、ｎCとｎが同ビット長の値である場合には、センタによる認証が可能になる。

【図面の簡単な説明】

【図１】生成される公開鍵（ｄ）の形態の一例を示す説明図。

【図２】本発明の実施例のシステム構成を示すブロック図。

【図３】図２のシステム構成において、生成される公開鍵（ｄ）の形態の他の例を示す説明図。

【図４】ユーザの計算機のハードウェア構成を示す説明図。

【図５】図４のハードウェア構成において生成される、非対称暗号鍵の生成を示すフローチャート。

【図６】図４のハードウェア構成において生成される、非対称暗号鍵の公開鍵（ｄ）の生成を示すフローチャート。

【図７】非対称暗号鍵の登録を示すフローチャート。

【図８】非対称暗号鍵を用いた暗号通信を行うための前処理を示すフローチャート。

【図９】従来例を示す説明図。

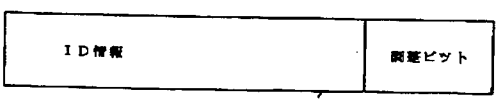
【図１０】従来例を示す説明図。

【符号の説明】

２００…通信網、２０１…計算機、２０５…計算機、２０９…ホスト。

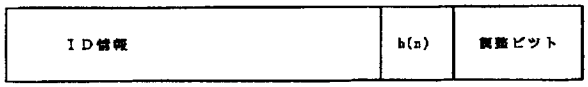
【図１】

図１



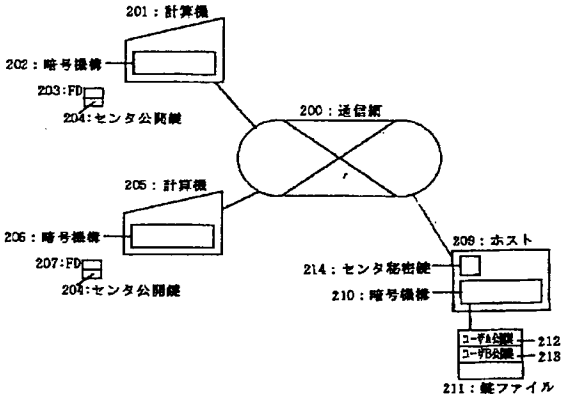
【図３】

図３



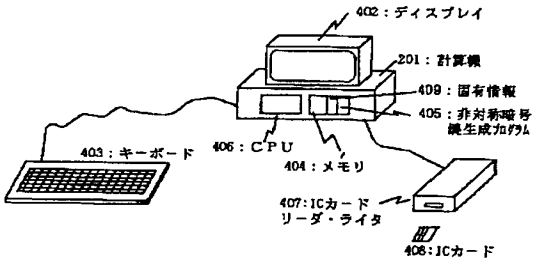
【図２】

図 2



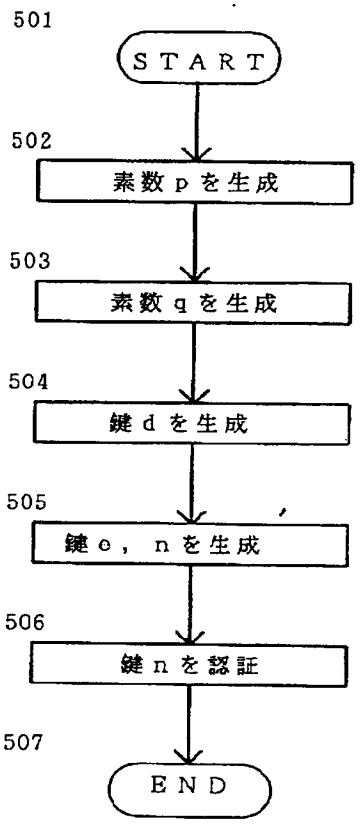
【図４】

図4



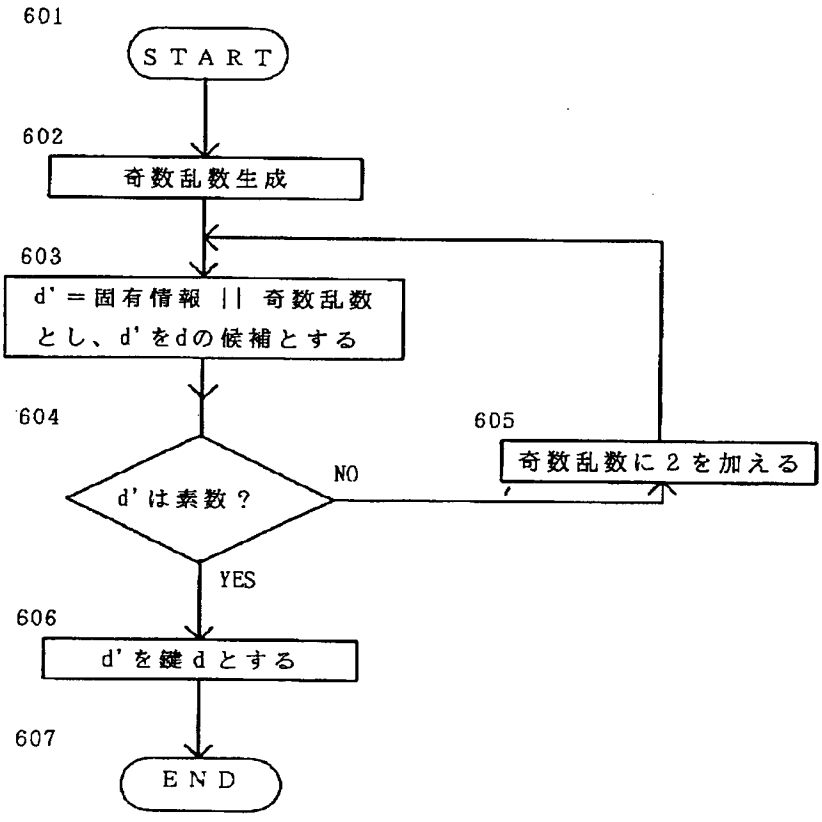
【図５】

図 5



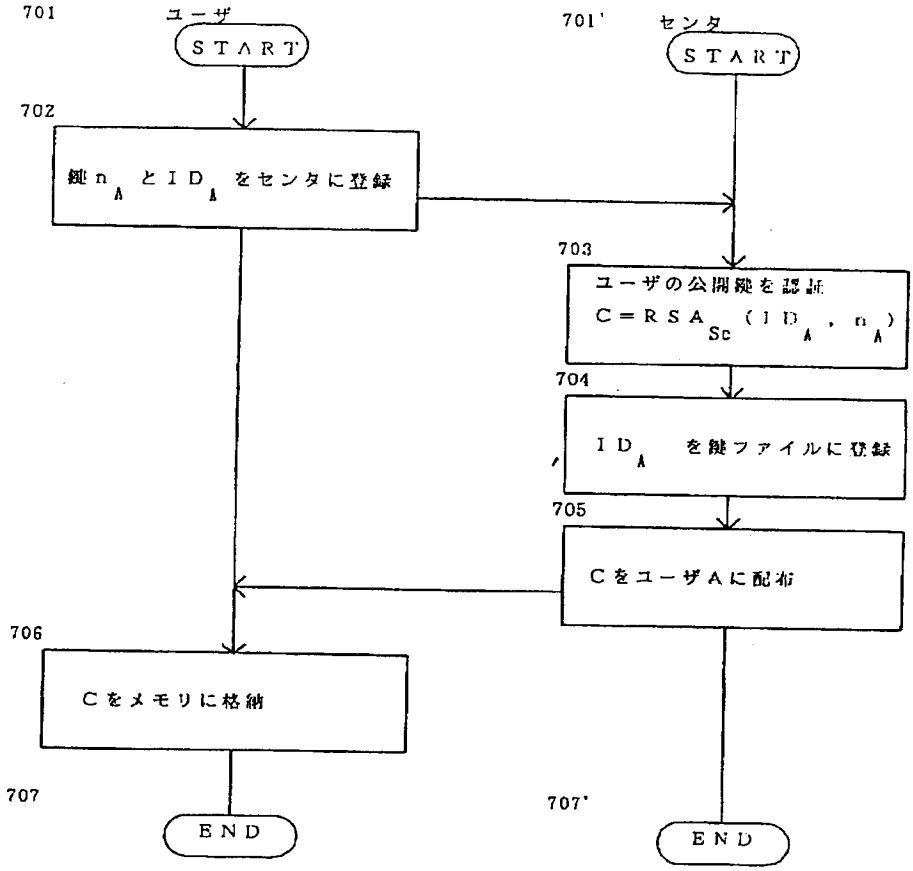
【図６】

図 6



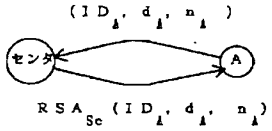
【図７】

図７



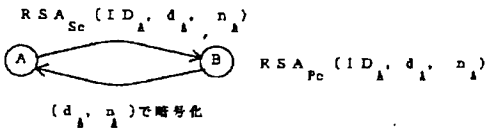
【図９】

図９



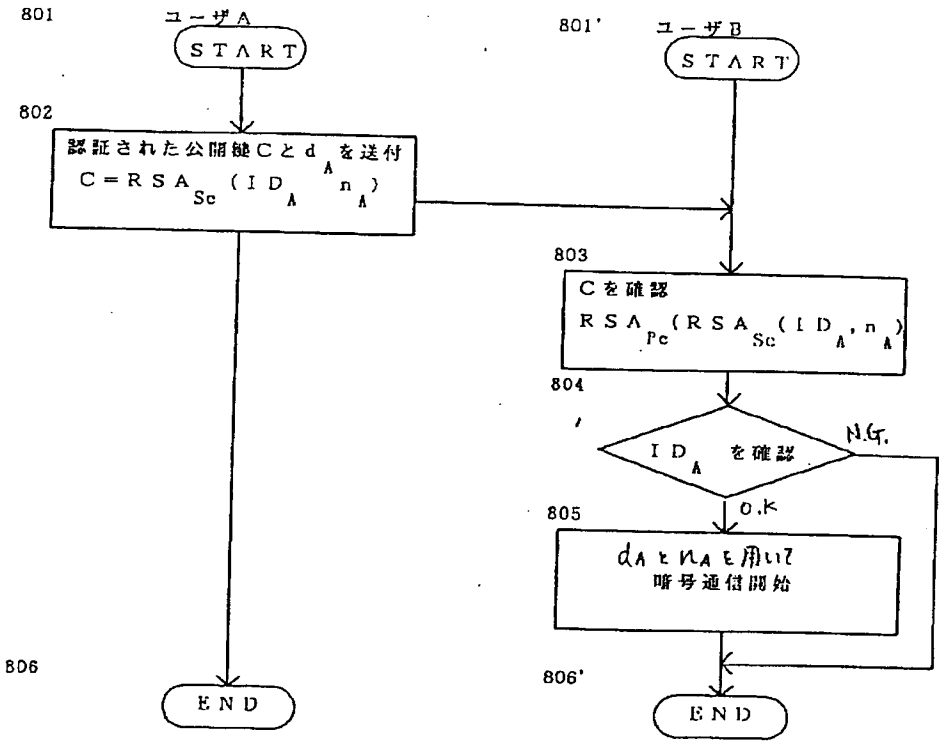
【図１０】

図１０



【図８】

図８



フロントページの続き

(51) Int. Cl. 5	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/14				

(72) 発明者　平野　秀一
神奈川県横浜市戸塚区戸塚町216番地　株式会社日立製作所情報通信事業部内